



WiMAX Forum X.509 CRL Profile Approved Specification

Version 1.0.1.

June 3rd, 2009

WiMAX Forum Proprietary

Copyright © 2008 WiMAX Forum. All Rights Reserved.

1 **Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability**

2
3 Copyright 2009 WiMAX Forum. All rights reserved.

4
5 The WiMAX Forum® owns the copyright in this document and reserves all rights herein. This document is available for
6 download from the WiMAX Forum and may be duplicated for internal use, provided that all copies contain all proprietary notices
7 and disclaimers included herein. Except for the foregoing, this document may not be duplicated, in whole or in part, or
8 distributed without the express written authorization of the WiMAX Forum.

9
10 Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance
11 of the following terms and conditions:

12
13 **THIS DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST**
14 **EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY**
15 **WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE,**
16 **NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX**
17 **FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND**
18 **DISCLAIMS ANY WARRANTIES TO THE CONTRARY.**

19
20 Any products or services provided using technology described in or implemented in connection with this document may be
21 subject to various regulatory controls under the laws and regulations of various governments worldwide. The user is solely
22 responsible for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all
23 required authorizations, permits, or licenses for its products and/or services as a result of such regulations within the applicable
24 jurisdiction.

25
26 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**
27 **APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY**
28 **OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.**

29
30 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**
31 **SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY**
32 **CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.**

33
34 The WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any
35 technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any
36 technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual
37 property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology,
38 standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies,
39 technologies, standards, and specifications, including through the payment of any required license fees.

40
41 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH**
42 **RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED**
43 **INTO THIS DOCUMENT.**

44
45 **IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO THE USER OR TO A THIRD**
46 **PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING,**
47 **WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY’S INTELLECTUAL**
48 **PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY**
49 **USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS**
50 **MEMBERS RELATING TO THE USE OF THIS DOCUMENT.**

51
52 The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion. The user is
53 solely responsible for determining whether this document has been superseded by a later version or a different document.

54
55 “WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum
56 Certified,” the WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks of the WiMAX Forum.
57 Third-party trademarks contained in this document are the property of their respective owners.

58

1 **Table of Contents**

2 **1. INTRODUCTION AND SCOPE 6**

3 1.1 Terminology 6

4 **2. REFERENCES 7**

5 **3. ABBREVIATIONS AND DEFINITIONS..... 8**

6 **4. ASSUMPTIONS 9**

7 **5. CERTIFICATE REVOCATION LISTS..... 10**

8 5.1 WiMAX CRL Profile 11

9 5.1.1 *WiMAX CRL Field Requirements* 11

10

11

1 **List of Figures**

2

3

1 **List of Tables**

2 TABLE 5-1 – FIELDS REQUIRED IN WIMAX CRL 11
3 TABLE 5-2 – CRL EXTENSIONS REQUIRED IN WIMAX CRLS 11

4

1 **Revision History**

December 18 th , 2007	Initial draft
April 2 nd , 2008	Updated title page, headers, and copyright year.
April 16 th , 2008	No changes. Published as Draft Specification Version 1.0.0.
June 3 rd , 2009	Updated references to 5480. Removed referencce to 3279. Added refernce to RFC 2119.

1. Introduction and Scope

The purpose of this document is to specify the format of the X.509 CRL. This format shall be used by Device CAs when they issue CRLs verified by WiMAX Forum® Servers and shall be used by Server CAs when they issue CRLs verified by WiMAX Forum® Devices.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described below, taken from IETF RFC 2119 [3].

Note that the force of these words is modified by the requirement level of the document in which they are used.

- MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

1 **2. References**

- 2 [1] RFC 5480, Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile.
- 3 [2] RFC 4055, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public
- 4 Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- 5 [3] RFC 2119, Key words for use in RFCs to Indicate Requirement Levels

1 **3. Abbreviations and Definitions**

- 2 CA Certification Authority
- 3 NIST National Institute of Standards and Technology
- 4 FIPS Federal Information Processing Standards
- 5 RFC Request for Comments
- 6 TBD To Be Defined
- 7 SS Subscriber Station
- 8 CRL Certificate Revocation List
- 9 SHA Secure Hash Algorithm
- 10 OID Object Identifier
- 11

1 **4. Assumptions**

- 2 Each SS need not attain WiMAX Forum Certified™ status. Such status can be determined by accessing public
3 information for the particular model number. For the purposes of this document and Release 1.0 network
4 specification, this issue is not particularly relevant. It is assumed that determination of such status and consequent
5 actions are outside the scope of the Release 1.0 Stage 2/3 specification.

5. Certificate Revocation Lists

This section describes the fields of CRLs issued by the WiMAX CAs.

The WiMAX certificate hierarchy assumes a two or three level tree that is rooted by two separate WiMAX Forum® Root CAs: a Device Root CA and a Server Root CA. The Device PKI has subordinate CAs for each of the device manufacturers (called Manufacturer CAs) and optionally, one more lower subordinate CA (called Device Sub-CAs) for each manufacturing site that may perform local issuance of certificates at the time of manufacture. Device certificates can be issued either from Manufacturer CAs or Device Sub-CAs. The Server PKI has subordinate CAs for each of the service providers (called Server CAs). All CAs in the both hierarchies MUST issue CRLs on the frequency documented in either the Device CP or Server CP, depending on whether the CA is a Device CA or Server CA.

WiMAX CRLs SHALL be constructed in accordance with IETF RFC 5480 [2] and the type definitions and default values provided in [2] are implicitly incorporated here except where explicitly overridden in this clause.

All of the following certificates have the following common attributes:

- All CRLs SHALL be version 2 X.509 certificates.
- The CA SHALL sign CRLs with SHA-256 with RSA encryption.

5.1 WiMAX CRL Profile

The WiMAX CRL format is defined in RFC 5480 [2], with additional requirements described in 5.1.1.

5.1.1 WiMAX CRL Field Requirements

A WiMAX CRL SHALL include the fields in Table 5-1.

Table 5-1 – Fields Required in WiMAX CRL

Field Name	RFC3280bis type	Value	Reference
<i>TBSCertList</i> {	SEQUENCE	CRL contents	N/A
<i>version</i>	INTEGER	v2	5.1.1.1
<i>signature</i>	AlgorithmIdentifier	See Error! Reference source not found.	Error! Reference source not found.
<i>issuer</i>	Name	Name of issuing CA	0
<i>thisUpdate</i>	Time	Date on which the CRL is issued	5.1.1.4
<i>nextUpdate</i>	Time	Date on which the next CRL will be issued.	5.1.1.5
<i>revokedCertificates</i> {	SEQUENCE OF	An entry for each revoked certificate	5.1.1.6
<i>userCertificate</i>	SerialNumber	SerialNumber of revoked	5.1.1.6.1
<i>revocationData</i>	Time	Date on which certificate was revoked	5.1.1.6.2
<i>crlEntryExtensions</i>	Extensions	Extension for this CRL entry	5.1.1.6.3
}			N/A
<i>crlExtensions</i>	Extensions	Extensions for the CRL	Table 5-1 and 5.1.1.7
}			N/A
<i>signatureAlgorithm</i>	AlgorithmIdentifier	See Error! Reference source not found.	5.1.1.8
<i>signatureValue</i>	BIT STRING	CRL Signature	5.1.1.9

The Extensions field SHALL contain the extensions shown in Table 5-2.

Table 5-2 – CRL Extensions Required in WiMAX CRLs

Extension Name	Critical	Contents	Reference
<i>authorityKeyIdentifier</i>	N	KeyIdentifier Equal to the issuer's subjectKeyIdentifier field	5.1.1.7.1
<i>crlNumber</i>	N	Indicates CRL number	5.1.1.7.2

A WiMAX CRL SHALL NOT include any additional critical CRL entry extensions or CRL extensions.

5.1.1.1 version

WiMAX CRLs SHALL be version 2.

5.1.1.2 signature

The *signature* field contains the the algorithm identifier for the algorithm used by the CA to sign the CRL.

1 The CA SHALL sign CRLs using the SHA-256 algorithm with RSA indicated with the OID
2 sha256WithRSAEncryption as defined in RFC 4055 [2] (PKCS#1 1.5).

3 **5.1.1.3 issuer**

4 The *issuer* field SHALL be the name of the issuer CA as required by and formatted as defined by RFC3280bis. See
5 section 3.1.1 of CP.

6 **5.1.1.4 thisUpdate**

7 The *thisUpdate* field specifies when this CRL was generated. It is either encoded as UTCTime, with the format:
8 YYMMDDHHMMSSZ, or GeneralizedTime, with the format: YYYYMMDDHHMMSSZ. If thisUpdate is in 2050
9 or later then GeneralizedTime must be used, otherwise UTCTime is used.

10 **5.1.1.5 nextUpdate**

11 The *nextUpdate* field specifies when the next CRL will be generated. It does not indicate when the CRL expires
12 because CRLs never expire. It is either encoded as UTCTime, with the format: YYMMDDHHMMSSZ, or
13 GeneralizedTime, with the format: YYYYMMDDHHMMSSZ. If thisUpdate is in 2050 or later then
14 GeneralizedTime must be used, otherwise UTCTime is used.

15 **5.1.1.6 revokedCertificates**

16 The *revokedCertificates* field specifies the revoked certificates. It contains zero or more ordered sequence, each
17 consisting of the fields listed below.

18 **5.1.1.6.1 userCertificate**

19 The *userCertificate* field indicates the serial number of the revoked certificate. The certificate serial number
20 SHALL be a string of up to 20 octets representing a non-negative integer.

21 **5.1.1.6.2 revocationData**

22 The *revocationDate* field indicates when the certificate was revoked. It does not indicate when the CRL expires
23 because CRLs never expire. It is either encoded as UTCTime, with the format: YYMMDDHHMMSSZ, or
24 GeneralizedTime, with the format: YYYYMMDDHHMMSSZ. If thisUpdate is in 2050 or later then
25 GeneralizedTime must be used, otherwise UTCTime is used.

26 **5.1.1.6.3 crlEntryExtensions**

27 The *crlEntryExtensions* field contains additional information about the revoked certificate. No CRL entry extensions
28 are required,

29 **5.1.1.7 crlExtensions**

30 The *crlExtension* field contains additional information about the CRL. The following two extensions are required.

31 **5.1.1.7.1 authorityKeyIdentifier**

32 The *authorityKeyIdentifier* extension SHALL be present.

33 The *authorityKeyIdentifier* extension SHALL be generated using RFC 5480 [2] 4.2.1.2 method 1 – the 160 bit SHA-
34 1 hash of the issuer's public key.

35 **5.1.1.7.2 crlNumber**

36 The *crlNumber* extension SHALL be present.

37 The *crlNumber* extensions convey a monotonically increasing sequence number for a given CRL scope and CRL
38 issuer.

39 **5.1.1.8 signatureAlgorithm**

40 The *signatureAlgorithm* field SHALL be identical to the signature field described in 5.1.1.2.

- 1 **5.1.1.9 signatureValue**
- 2 The RSA key length SHALL be at least 2048 bits.